Criminal

Live links in the Crown court

Richard Hearnden sets out the case for greater use of cheaper, off-the-shelf systems in the crown court without recourse to changes in the law

The publication of *Transforming Our Justice System,* by the Ministry of Justice, the Lord Chief Justice and the Senior President of Tribunals in September 2016, marks another milestone on the road to the digitisation of court proceedings. The paper promises that 'the revolution in technology will characterise tomorrow's justice system'.

Criminal practitioners will be familiar not so much with tomorrow's innovations, but rather with the mixed innovations made in the last decade to the crown court estate. One noticeable innovation has been the heavy investment in technology designed to make it easier for people to participate in court proceedings remotely. But has this investment been worth it? And is there a cheaper way of live linking a court, perhaps by using an off-the-shelf system like Skype or FaceTime?

Despite Lord Thomas of Cwmgiedd in his first press conference as Lord Chief Justice calling for the use of Skype and FaceTime in pre-trial proceedings, a common myth abounds that such off-the-shelf systems are not permitted. This myth seems to apply to criminal and civil courts.

In *Re ML (Use of Skype Technology)* [2013] EWHC 2091 (Fam), Peter Jackson J expressed concern in an adoption case that Skype without a 'bridging system' had 'issues about security'. Anecdotal evidence exists of courts insisting that only the court-supplied system may be used for a live television link. But, as observed in *Re ML*, these systems are costly. These costs can range from a few hundred to many thousands of pounds, depending on the location of the witness and the length of the link. The rationale for not permitting Skype or FaceTime is that neither system is secure enough.

Why does a live link need to be encrypted? Isn't oral testimony in the crown court given in public, where anyone can come along and watch? One explanation supporting the security theory (as told by one court officer) is that an unscrupulous third party could hack into the line and make a recording of the evidence. As it will be shown, off-the-shelf systems possess superior security features that far exceed anything required in law. Indeed, communication security does not appear as a prerequisite for live linking anywhere in the Criminal Procedure Rules.

Legal basis for live links

The ability of the crown court to receive evidence other than from the witness box is prescribed in statute. This was made clear in a line of recent authorities of the Court of Appeal (Criminal Division). In *R v Diane* [2010] 2 Cr App R 1, *R v Hampson* [2014] 1 Cr App R 4 and *R v Clark* [2016] 1 Cr App R (S) 52, the court found that evidence received by *telephone* was inadmissible.

The reasoning was that Parliament had legislated to permit live television links and to permit a witness's

statement to be read into evidence, but it had not legislated to allow evidence to be given in the crown court over the telephone. The court found there was no basis for admitting it other than a statutory one. In *Hampson*, the court found itself constrained by the decision in *Diane* to hold that the power to receive evidence was regulated by statute. The court held:

'In the light of the decision in *Diane*, we consider that the power of the courts in criminal cases to receive evidence other than by a person being present to give oral evidence is regulated by statute.'

In *Hampson*, a witness in a case of causing death by dangerous driving was unable to attend the trial in Liverpool because he was on an oil rig. The Court of Appeal lamented the failure of the crown court to take evidence from the witness him by way of Skype. The trial judge had been informed that 'there was no way' this could be used but it seems no substantial enquires had been made with the employer. The court said:

'We do not believe [the employer] would do anything, in a case of this kind, other than to assist the interests of justice by making either a facility over Skype available or, better still, their video conferencing.'

So, telephone evidence and any evidence received other than as provided by statute is not permitted. And here the Court of Appeal has *hinted* at the use of off-the-shelf systems, with Skype specifically suggested. So what is the position?

> The bill that became the CJA 2003 cleared all its Commons committee stages about six months before Skype was even invented. But, surprisingly, the explanatory notes to the Act anticipated the availability of an internet-based system

Live links under CJA 2003, s 51

First, s 51 of the Criminal Justice Act 2003 (CJA 2003) provides for the use of domestic live links, where the court so directs, and s 32 of the Criminal Justice Act 1988 governs international live links. The CJA 2003 permits live links where it is in the interests of the 'efficient or effective administration of justice' and 'it has been notified by the Secretary of State that suitable facilities for receiving evidence through a live link are available in the area in which it appears to the court that the proceedings will take place'. The earlier legislation is less proscriptive and simply requires the leave of the court.

One assumes the purpose behind the notification provisions introduced later was that the court itself then was embarking on a programme of equipping courts to receive this evidence, rather than it being for the parties to make the arrangements themselves. The interpretation of a 'live link' is provided for by s 56 (2) of the CJA 2003:

'a live television link or other arrangement by which a witness, *while at a place in the United Kingdom* which is outside the building where the proceedings are being held, is able to see and hear a person at the place where the proceedings are being held and to be seen and heard by the [participants in court].'

There is nothing there about it having to be encrypted. What was Parliament contemplating when these provisions were debated?

The Bill that became the CJA 2003 cleared its Commons committee stages about six months before Skype was invented. But, surprisingly, the explanatory notes to the Act anticipated the availability of an internet-based system, such as Skype:

'"Live link" is defined in s 56(2) and will usually mean a closed circuit television link, but could apply to any technology with the same effect such as video conferencing facilities or the internet.'

The two-stage test in s 51

In cases where a witness is unavailable or physically unable to attend court in person, it will almost always be in the interests of the efficient or effective administration of justice to receive their evidence by live link. But what about the notification by the Lord Chancellor? Again, the explanatory notes offer some assistance:

'... this will allow for phased implementation of the facilities required for live links. The responsibility for ensuring that there are facilities in the remote location from which the witness intends to give evidence falls to the parties and is therefore not covered by this section.'

So, nothing there about, for instance, the live link being allowed only on an approved, encrypted system. Indeed, if that were to have been the case, Parliament would have expressly said so.

Finally, what do the Criminal Procedure Rules 2015 have to say on the matter? As purely secondary legislation, the CrimPR incorporates the statutory framework and is not reproduced in this article. Readers can find the relevant provisions under rules 18.23 to 18.26. It follows that where the necessary notification has been given, where the court's permission has been gained and, where necessary, the party calling the witness shows it is in interests of the efficient or effective administration of justice and the Lord Chancellor has certified that the facilities exist, an off-the-shelf system may be used.

Security concerns

Are off-the-shelf systems secure? According to industry experts, yes (*Computer Weekly*: *http://bit.ly/2dF6P57*). FaceTime and Skype use widely trusted encryption techniques. RSA, an industry standard encryption key, is used for the 'handshake' required to connect a call. A secret digital key is created which is transmitted automatically by the caller to the recipient. If it is intercepted, it cannot be decrypted because only the recipient, using a second private key, is able to decode it. Criminal Justice Secure Mail (CJSM) uses a similar method. But the FaceTime or Skype call itself is further scrambled using 256-bit AES encryption technology which is no less secure and possibly offers an even greater level of encryption than that used by CJSM (see: *http://bit.ly/2fb7ccA*). Any eavesdropper would, in theory, find it impossible to intercept a call made using Skype or FaceTime. So, the reported objections to these systems fail on both grounds: they are adequately encrypted and far more so than the law requires them to be.

Court users should beware of being too bold, as counsel were in *Hampson* and other cases where evidence was given over the telephone. But the writer's view is that there is no reason why clients should have to shell out, or legal aid applications made to pay for, the expensive official system. ●

Contributor **Richard Hearnden**, Furnival Chambers